MATH 115, SUMMER 2012
LECTURE 12

JAMES MCIVOR

- last time - we used hensel's lemma to go from roots of polynomial equations mod p to roots mod p^2, mod p^3, etc.
- from there we can use CRT to construct roots for other composite moduli
- we review this procedure in the problem session
- today we want to know how to solve polynomial congruences mod p

1. Solving Congruences mod p

- Question: is there a general way to attack the solution of congruences mod p, where p is prime?
- No. This can be a hard problem.
- if the prime is small, can just guess and check for solutions.
- But the first thing to ask is: are there any solutions at all?
- If no sol'ns mod p, then no soln's mod m either:

Lemma 1. *If the congruence $f(x) \equiv 0 \mod m$ has no solution mod p, where p is a prime factor of m, then it has no solutions mod m either.*

Proof - use CRT.

IMPORTANT - to find the degree of the congruence, you must first reduce the coefficients of f mod p -

- some of the coefficients may drop out and the degree will be lower than the original degree of f as a polynomial. In particular, when we say a congruence "has degree n", we mean that it is not zero mod p.

Next question, what's the max number of sol'ns? Answer: the degree of the congruence, or infinity

Key observation: every integer is a solution to the congruence $x^p - x \equiv 0$. This is just Fermat's Thm. So the polynomial $x^p - x$ is "bad" when we work mod p. The idea of the following results is to first divide out any copies of this "bad" polynomial.

The first theorem says we can limit our attention, when working mod p, to congruences of degree less than p.

Proposition 1. *Let $f(x) \equiv 0 \mod p$ be a congruence of degree n. If $n \geq p$, then one of two things can happen:*

(1) *Every integer is a solution of the congruence, or*
(2) *There is another congruence $g(x) \equiv 0 \mod p$, with leading coefficient one and degree less than p, whose solutions are the same as those of $f(x) \equiv 0 \mod p$.*

Proof. Define the "bad" polynomial $b(x) = x^p - x$. We use long division for polynomials, dividing f by b:

$$f(x) = q(x)b(x) + r(x),$$

where the degree of $r(x)$ is less than p (the degree of b).

- NOTICE - $f(x)$ and $r(x)$ have the same roots, since everything is a root of b.
- 2 cases

(1) $r(x) = 0 \mod p$ (this means either $r(x) = 0$ or every coefficient is divisible by p. Here everything is a solution.
(2) The solutions of $f(x) \equiv 0 \mod p$ are the same as those of $r(x) \equiv 0 \mod p$, which has degree less than p. Can make leading coefficient 1 by multiplying through by the inverse of the leading coefficient (remember that $\mathbb{Z}/p$ is a field).

□

Proposition 2. *If the congruence $f(x) \equiv 0 \mod p$ has degree $n < p$, then there are at most n solutions.*

Proof. - First write $f(x) = a_n x^n + \ldots + a_1 x + a_0$. After reducing mod p, we assume that $p \not| a_n$, so this congruence has degree n.

We do induction on n. The case $n = 0$ corresponds to the "constant" congruence $f(x) = a$, and by our assumption, $p \not| a$. So there are $0 (= n)$ solutions. For $n = 1$, we have a linear congruence $ax + b \equiv 0 \mod p$. Since $p \not| a$, a has an inverse, and we get a unique solution $x \equiv -b \cdot a^{-1} \mod p$.

Now assume we've proven that every congruence of degree k less than n has at most k solutions. We'll prove it when $k = n$. We use contradiction - assume there are distinct solutions $x_1, \ldots, x_{n+1}$.

- write $f(x) = a_n x^n + \ldots + a_1 x + a_0$, and define a new polynomial

$$g(x) = f(x) - a_n \prod_{i=1}^{n} (x - x_i)$$

- the degree n terms cancel, so g has degree less than n, or has no degree, meaning it's zero mod p. Each $x_1, \ldots, x_n$ is a solution.

- by induction, if it has a degree, it can't have n solutions, so it must be the zero congruence (i.e., every integer solves it). But then in particular x_{n+1} solves it, so

$$f(x_{n+1}) \equiv 0 \equiv a_n (x_{n+1} - x_1) \cdots (x_{n+1} - x_n) \mod p,$$

and this is a contradiction since the x_i are all distinct mod p. □

Remark 1. The book talks about congruences "having a degree" and it's a bit confusing. They say a polynomial *does not* have a degree when p divides all the coefficients. I've tried to stick to their terminology. But I think a better way to think about congruences mod p (or mod m even when m is not prime) is to think of the coefficients as elements of the ring $\mathbb{Z}/p$. Then a polynomial doesn't have a degree exactly when all of its coefficients are zero (in the ring $\mathbb{Z}/p$). This is consistent with more familiar terminology - for polynomials with real coefficients, we don't usually assign a degree to the zero polynomial (the reason for this is that it has infinitely many roots, and we want to say that degree n polynomials have at most n roots).

This point of view is the content of Theorem 2.28 in your book, although they don't really explain that theorem very well.

Now, to finish our discussion of the number of sol'ns of $f(x) \equiv 0 \mod p$, we ask: when do they have *exactly* n solutions? The answer, basically, is: when f divides the bad polynomial mod p! This means that there is another polynomial $q(x)$ such that $b(x) \equiv q(x)f(x) \mod p$ for all integers x.

Proposition 3. *Let $f(x) \equiv 0 \mod p$ be a congruence of degree n. It has exactly n solutions if and only if f divides $b(x) = x^p - x$ mod p.*

Proof. - First assume it has n solutions ($n \leq p$, since there are only p elements in $\mathbb{Z}/p$).

- Long division:

$$x^p - x = f(x)q(x) + r(x),$$

where r has degree less than n or else is zero mod p.

- since every integer is a root of b, the solutions of f must also be sol'ns of r (but not conversely - q has roots too!) So r has at least as many solutions as f, so it must be zero mod p. Thus f divides b mod p.

- Other direction. If f divides b mod p, we have

$$b(x) = x^p - x \equiv f(x)q(x) \mod p$$

- now count solutions

- since everything is a root of b, there are p solutions to $f(x)q(x) \equiv 0 \mod p$.

- f and q are both **monic**, i.e., have leading term 1, so the congruences $f \equiv 0$ and $q \equiv 0$ have at most n and $p - n$ solutions, respectively (need monic to make sure they have these degrees mod p)

- roots of b are all either roots of f or roots of q. Specifically, b has p roots mod p. Let a be one of them, so that $f(a)q(a) \equiv 0 \mod p$. Then $f(a)q(a)$ is a number with the property that $p|f(a)q(a)$. Since p is prime, p divides one or the other. So a must be a root of either f or q mod p. Thus each root of b is a root of one of the two factor, so all the roots of b appear as the roots of f and q,

- f and q must therefore have the full n and $p - n$ roots, respectively. So f has n roots, like we wanted.

□

Example 1.1. What about the simple polynomial $x^d - 1$. How many roots does it have mod p? We might hope that it has d roots. The previous prop says that's true if it divides $x^p - x$.

Now do some algebra tricks:

$$(x^d - 1)(1 + (x^d) + (x^d)^2 + \cdots + (x^d)^{n-1}) = (x^d)^n - 1 = x^{dn} - 1$$

Multiply both sides by x:

$$x(x^d - 1)(1 + (x^d) + (x^d)^2 + \cdots + (x^d)^{n-1}) = x^{dn+1} - x$$

This holds for all $n > 1$. We want the right side to be $x^p - x$, so just take $dn+1 = p$. Of course this is only possible if d divides $p - 1$.

Conclusion: when $d|p - 1$, the polynomial $x^d - 1$ has exactly d roots mod p.

Problem Session

2. Reduction of Modulus

If we want to solve a congruence of the form

$$f(x) \equiv 0 \mod m$$

we now have all the tools needed to reduce to the case where m is actually prime. Let's first review this process, and then consider what can be said when m is prime.

First, suppose that m has the factorization

$$m = \prod_{i=1}^{r} p_i^{a_i},$$

where the p_i are prime. Now the numbers $p_1^{a_1}, \ldots, p_r^{a_r}$ are pairwise relatively prime, so by the CRT, the solutions x mod m are in bijection with r-tuples of solutions $(x_1, \ldots, x_r)$, where each x_i is a solution of

$$f(x) \equiv 0 \mod p_i^{a_i}$$

Alternatively, we can think of this step in the following way. Solving the expression $f(x) \equiv 0 \mod m$ is the same thing as asking: "which elements of the ring $\mathbb{Z}/m$ satisfy the equation $f(x) = 0$?" By the CRT, the ring $\mathbb{Z}/m$ is isomorphic to the product ring $\mathbb{Z}/p_1^{a_1} \times \cdots \times \mathbb{Z}/p_r^{a_r}$, so this is the same as asking which elements of the ring $\mathbb{Z}/p_1^{a_1} \times \cdots \times \mathbb{Z}/p_r^{a_r}$ satisfy the given equation. But elements of this product ring look like $(x_1, \ldots, x_r)$, and the expression $f(x) = 0$ becomes in this ring $f(x_1, \ldots, x_r) = (f(x_1), \ldots, f(x_r)) = (0, \ldots, 0)$.

Thus it suffices to consider each prime power factor $p_i^{a_i}$ separately, and when we've solved these, we just multiply them together to get our solutions mod m.

Now, how do we reduce from a prime power factor to a prime factor? This is Hensel's lemma. It says that if we have a solution mod p, and the solution is nonsingular, we can lift it to a unique solution mod p^2, mod p^3, etc. So once we have the solutions mod p_i, for each i, we can lift them up to the required prime power factors $p_i^{a_i}$, and then we'll be done.

Let's look at an explicit example.

Example 2.1. Consider the congruence $x^2 + x + 1 \equiv 0 \mod 3025$. Use the prime modulus solutions $x \equiv 1 \mod 5$ and $x \equiv 4 \mod 13$ to construct a solution mod 3025.

solution: We do this in steps:

(1) Factor $m = 3025$, namely $3025 = 5^2 \cdot 11^2$.
(2) Check that the solutions are nonsingular. The derivative is $2x + 2$. Mod 5, we have $2(1) + 2 \not\equiv 0 \mod 5$, and mod 13, we have $2(4) + 2 = 10 \not\equiv 0$ mod 13, so they're both nonsingular.
(3) Lift the mod 5 solution to a solution mod 5^2. Remember from last lecture that we first have to find a multiplicative inverse to $f'(a_1)$, where here $a_1 = 1 \mod 5$. Since $f'(1) = 4 \mod 5$, 4 is the inverse (reason: $4 \cdot 4 = 16 \equiv 1 \mod 5$). Thus from the formula from last lecture, we get $a_2 = a_1 - f(a_1)f'(a_1)^{-1} = 1 - 5 \cdot 4 = -19 \equiv 6 \mod 5^2$.
(4) Lift the mod 13 solution. Here $a_1 = 4 \mod 13$, and $f'(a_1) = 10$, with inverse 4, so $a_2 = a_1 - f(a_1)f'(a_1)^{-1} = 4 - 26 \cdot 4 = 4 - 104 = -100$ mod 13^2

(5) Now we have the prime power solutions $x \equiv 6 \mod 25$ and $x \equiv -100 \mod 169$. To get the solution mod $4225 = 25 \cdot 169$ we apply the CRT isomorphism

Example 2.2 (Singular roots)**.** We won't worry about singular roots too much, but just give an example to show that the uniqueness of lifting may fail - we may be able to lift a root mod p^j to *many* roots mod p^{j+1}, or we may not be able to lift it at all!

Let's try to solve $f(x) = x^2 - 3x + 1 \equiv 0 \mod 25$. We first work mod 5, and get the solution $a_1 \equiv 4 \mod 5$. We have $f'(4) = 5 \equiv 0 \mod 5$, so this root is singular. Look at the Taylor series:

$$f(a_1 + tp) = f(a) + tpf'(a) + t^2p^2f''(a)/2! \mod p^2$$

The degree two term would vanish even if the root were nonsingular, as we saw in the proof. The problem with singular roots is that even the first-order term vanishes! Because if $f'(a) \equiv 0 \mod p$, then $pf'(a) \equiv 0 \mod p^2$. In the nonsingular case, we look for a value of t. We do that here, too, but one of two things happens: 1) every value of t works (we only need consider t mod p), or 2) No value of t works.

Let's see how it goes for this example. We have $f(4+5t) \equiv f(4) \mod 5^2$. So we will find many values of t that work if and only if $f(4) \equiv 0 \mod 5^2$ (of course, we already know 4 is a root mod 5, the question is whether it's also a root mod 25). Well, $f(4) = 5$, which is not congruent to zero mod 25. So our root mod 5 *doesn't* lift to a root mod 25...